

Media Contact:

Will Wiquist
will.wiquist@fcc.gov

For Immediate Release

FCC PRIVACY & DATA PROTECTION TASK FORCE LAUNCHES FIRST-EVER ENFORCEMENT PARTNERSHIPS WITH STATE ATTORNEYS GENERAL

MOUs Signed with Four States with More Welcomed to Join

WASHINGTON, December 6, 2023—FCC Chairwoman Jessica Rosenworcel today announced a new initiative to strengthen and formalize the cooperation between the Commission and its State partners on privacy, data protection, and cybersecurity enforcement matters. As part of the work of the FCC’s Privacy and Data Protection Task Force, the agency’s Enforcement Bureau has signed Memoranda of Understanding (MOU) with the Attorneys General of Connecticut, Illinois, New York, and Pennsylvania to share expertise, resources, and coordinated efforts in conducting privacy, data protection, and cybersecurity-related investigations to protect consumers.

What’s New?

The new Memoranda of Understanding affirm that the FCC and State Attorneys General “share close and common legal interests in working cooperatively to investigate and, where appropriate, prosecute or otherwise take enforcement action in relation to privacy, data protection, or cybersecurity issues” under sections 201 and 222 of the Communications Act. Coordinated action and information sharing will take place under all applicable Federal and State laws and privacy protections.

Federal and State Leaders

FCC Chairwoman Jessica Rosenworcel said: “Defending consumer privacy is an all-of-government responsibility and a shared challenge. Today we take on evolving consumer threats with new formal partnerships with state law enforcement leaders, which have already been successful in obtaining record-breaking results in combatting illegal robocalls. I am thankful to these four partners for prioritizing interagency cooperation, and we welcome other state leaders to join us in this effort to ensure we work together to protect consumers and their data.”

FCC Enforcement Bureau Chief Loyaan A. Egal said: “Use of information and communications technology and services have significantly enhanced our lives while at the same time increasing vulnerabilities to our privacy and sensitive data. These strategic partnerships with the Connecticut, Illinois, New York, and Pennsylvania Attorneys General Offices will allow us to maximize our efforts to address risks arising from the misuse or mishandling of sensitive data we entrust with service providers and the continued threats posed by cybercriminals and foreign adversaries.”

Connecticut Attorney General William Tong, Co-Chair of the of the National Association of Attorneys General’s (NAAG) Internet Safety/Cyber Privacy and Security Committee, said: “The Connecticut Office of the Attorney General was the first nationwide to form a dedicated privacy department in 2015. This work, in coordination with state attorneys general nationwide, has

remained a core priority of our office since then. Consumers have a right to know and control how their personal information is used, stored, and protected, and companies who violate that trust must be held accountable. This powerful new partnership between our states and the Federal Communication Commission is a recognition of the growing importance of this critical work.”

Illinois Attorney General Kwame Raoul, Co-Chair of the NAAG’s Consumer Protection Committee, said: “I am proud to work with the FCC to safeguard the private information of Illinoisans,” said Illinois Attorney General Kwame Raoul. “Similar state and federal partnerships have allowed us to successfully target perpetrators of illegal robocalls. This initiative gives Illinois access to more resources for investigating and holding accountable bad actors who fail to protect or misuse personal information.”

New York Attorney General Letitia James said: “As we see cybersecurity threats growing and evolving, we have a responsibility to do everything within our power to protect consumers and their personal information. This partnership between state and federal enforcement leaders will help strengthen our ability to protect consumers’ privacy and hold companies that violate the law accountable. I am proud to join my fellow attorneys general in this effort with the FCC to keep consumers safe.”

Pennsylvania Attorney General Michelle A. Henry said: “Every day millions of people have their personal information and data stolen or misused, or their data is not sufficiently protected. My Office’s partnership with the FCC will allow us to offer better online data protections for all Americans, including Pennsylvanians. Our formal agreement to pool our resources will better enable investigators to tackle a complicated and constantly evolving issue, giving us an advantage in our mission to hold those who break our laws accountable. We are excited to collaborate with the FCC and to utilize the resources they are providing through this partnership.”

Power of Partnerships

During investigations, both the FCC’s Enforcement Bureau and state investigators seek records, talk to witnesses, interview targets, examine consumer complaints, and take other critical steps to build a record against possible bad actors. These new partnerships can provide critical resources for building cases and coordinating efforts to protect consumers and businesses nationwide.

The FCC offers partner states not only the expertise of its enforcement staff but also important resources and remedies to support state investigations. For example, the MOUs may facilitate relationships with other authorities in this space including other federal agencies, and support for and expertise with critical investigative tools including subpoenas and confidential response letters from suspected targets. The FCC’s unique position and authorities have allowed the Commission to work with State partners to obtain measurable results in the robocalling space to scale efforts to protect consumers.

FCC’s Privacy and Data Protection Task Force

To lead and coordinate this important work, Chairwoman Rosenworcel created the Privacy and Data Protection Task Force to work on privacy and data protection issues subject to the Commission’s authority under the Communications Act. The Task Force coordinates across the agency on the rulemaking, enforcement, and public awareness needs regarding privacy and data protection activities, including threats like SIM swapping scams, port-out fraud, and data breaches, which can increase the risk posed by these scams by exposing consumers’ information that can make it easier for scammers to steal consumers cell phone accounts.

###

*This is an unofficial announcement of Commission action. Release of the full text of a Commission order constitutes official action.
See MCI v. FCC, 515 F.2d 385 (D.C. Cir. 1974).*